



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/751,038	12/31/2003	Eric Boyd	324212003110	1932
20872 7590 11/26/2007 MORRISON & FOERSTER LLP 425 MARKET STREET SAN FRANCISCO, CA 94105-2482			EXAMINER DINH, MINH	
			ART UNIT 2132	PAPER NUMBER
			MAIL DATE 11/26/2007	DELIVERY MODE PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/751,038	Applicant(s) BOYD ET AL.	
	Examiner Minh Dinh	Art Unit 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 September 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-4, 6, 12-14, 17, 21-25, 29, 32, 33 and 37-39 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☒ Claim(s) 3, 21, 25, 33 and 37 is/are allowed.
- 6) ☒ Claim(s) 1-2, 4, 6, 12-14, 17, 22-24, 29, 32 and 38 is/are rejected.
- 7) ☒ Claim(s) 39 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 December 2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

Response to Amendment

1. This action is in response to the amendment filed 09/07/07. Claims 1, 3-4, 12, 14, 17, 21-22, 25, 29, 32-33 and 37-39 have been amended; claims 5, 7-11, 15-16, 18-20, 26-28, 30-31, 34-36 and 40 have been cancelled.

Response to Arguments

2. Applicant's arguments filed 09/07/2007 have been fully considered but they are not persuasive.

Applicant argues that Beach discloses generating a single check digit may even discourage a programmer of ordinary skill from thinking of the use of a larger, multi-digit value of size $m \geq 16$ bits, such as a cryptographic hash code (page 16, 1st paragraph). One of ordinary skill in the art could recognize that Beach's single check digit generated by adding all digits of a number together cannot detect if a number has been modified (e.g., the easiest way to defeat the single check digit is to change the order of the digits to generate a new number). On the other hand, Schneier discloses that, with a cryptographic hash code, one can detect a single-bit change of the pre-image. It would have been obvious to one of ordinary skill in the art

to modify Beach's method to use a cryptographic hash code, as taught by Schneier, to be able to detect any modification to data.

Applicant argues that Schneier ("Applied Cryptography") is silent as to the length of the hash value, and does not disclose a hash value of size $m \geq 16$ bits (page 16, 2nd paragraph). Schneier, in Section 2.4, page 31, discloses in general that a message authentication code (MAC) can be generated using either a hash function or a block encryption algorithm, and refers to Section 18.14 for more discussions of MACs, in which Schneier further discloses various algorithms for generating a MAC value of size $m \geq 16$ bits (pages 455-459).

Claim Rejections - 35 USC § 112

3. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

4. Claims 1-3 and 6 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. Claim 1 recites the limitation "if valid then crediting the

user with the value indicated by the decrypted code.” (last line). Whereas the originally filed specification discloses crediting the user with a number of points associated with the code (page 93, paragraph 330), it does not disclose crediting the user with the value indicated by the code. For prior art rejection purpose, the limitation is interpreted as “if valid then crediting the user with the value associated with the decrypted code.” Claim 3 is rejected on the same basis as claim 1.

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-3 and 6 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 1, starting at line 4, recites the limitation “the encrypted code obtained by **appending** a third string, which is an output of applying an encryption algorithm employing a second secret code to a second string composed of an n-bit raw number and an m-bit validation number, wherein m is at least 16, the m-bit validation number generated by hashing, via a hash function, a first string, the first string composed of the n-bit raw number and the first secret code”. It is not clear from the claim language to which the third string is appended. For prior art rejection purpose, the limitation is interpreted as “the encrypted

code being an output of applying an encryption algorithm employing a second secret code to a second string composed of an n-bit raw number ..."

Claim 3 is rejected on the same basis as claim 1.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 1, 4 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Beach et al. (5,892,827) in view of Schneier ("Applied Cryptography"). Beach discloses a method for generating an authorization code, i.e., a PIN, to be printed on a coupon/award certificate and validating the authorization code when it is redeemed by a user (Abstract; col. 11, line 12 – col. 12, line 13).

Regarding claim 1, Beach specifically discloses a method for verifying the validity of an encrypted generated in base $L = 10$ (10 digits from 0-9) comprising:

obtaining an encrypted code from a user, the encrypted code generated by producing a first string through application of a checksum

function to the n-bit raw number, designating an m-bit portion of the first string as an m-bit validation number, i.e., the check digit, producing a second string through combination of the m-bit validation number and the n-bit raw number, producing a third string through application of an encryption algorithm to the second string with a secret key, and converting the third string to the base L string;

converting the encrypted code to a base 2 string (computers only recognize 0s and 1s);

decrypting the base 2 string using the secret key;

verifying the validity of the encrypted code by processing the decrypted base 2 string; and

if valid, then crediting the user with a value associated with the decrypted code (fig. 3; col. 6, line 56 – col. 8, line 32).

Beach discloses using a checksum function to generate the validation number. Beach does not disclose using a one-way hash function with a first secret key. Schneier discloses using a one-way hash function with a first secret key to generate a validation number having at least 16 bits (i.e., a MAC code) (pages 30-31, 455-459). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Beach method to use a one-way hash function with a first secret key to generate the validation number, as taught by Schneier. The motivation for doing so

would have been that: (i) given a hash value, it would be computationally unfeasible to find a pre-image that hashes to that value (page 30, last paragraph); (ii) only someone with the secret key could verify the hash value (page 31, 2nd paragraph); and (iii) one could detect a single-bit change of the pre-image (page 30, last paragraph).

Regarding claim 4, Schneier further disclose using MD5 algorithm for the keyed-hash function (page 456, table 18.2).

Regarding claim 6, Beach discloses that m is the least significant bit (LSB) portion of the first/second string. Beach does not disclose that m is the most significant bit (MSB) portion of the first/second string. At the time the invention was made, it would have been obvious to one of ordinary skill in the art to modify the encrypted code of Beach such that m is the most significant bit (MSB) portion of the first/second string. Applicant has not disclosed that assigning m to be the MSB portion of the first/second string provides an advantage, is used for a particular purpose, or solves a stated problem. One of ordinary skill in the art, furthermore, would have expected Applicant's invention to perform equally well with m being the least significant bit (LSB) portion of the first/second string as disclosed in the prior art because they serve the same purpose and one is just the alternative to the other. Therefore, it would have been obvious to one of ordinary skill in the art to modify Beach to obtain the invention as specified in claim 6.

9. Claim 2 is rejected under 35 U.S.C. 103(a) as being unpatentable over Beach in view of Schneier as applied to claim 1 above, and further in view of "FIPS PUB 46-3 – Data Encryption Standard (DES)" (hereinafter "FIPS 46-3"). Beach discloses encrypting and decrypting the code (fig. 3, step 50). Beach does not disclose using the DES3 algorithm. "FIPS 46-3" discloses using the DES3 algorithm, i.e., Triple DES algorithm (Section 15 – Qualifications). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the combined method of Beach and Schneier to use the DES3 algorithm for encryption and decryption, as taught in "FIPS 46-3", in order to increase data security (page 5, last paragraph).

10. Claims 12, 14, 17, 22, 24, 29, 32 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leason (6,251,017) in view of Beach and Schneier. Leason discloses a method and system for on-line validation of redeemed rewards which have been obtained off-line (Abstract).

Regarding claim 12, which represents claims 17, 22, 29 and 38, Leason discloses a method for verifying the validity of a code obtained by a user from an object, comprising the steps of:

receiving the code on-line from the user, the code is generated as a base L string and obtained by the user off-line from the object; converting the base L string to a base 2 string; verifying the validity of the code by processing the base 2 string; and awarding incentive points to the user if the code is valid (figures 3, 5-6, 11-12; col. 2, line 63 – col. 3, line 7; col. 5, lines 41-53; col. 6, lines 1-11).

Leason does not explicitly disclose that the code is generated by providing a number portion, deriving a validation portion from the number portion, appending the validation portion to the number portion to form a string, encrypting the string, and deriving the code from the encrypted string by converting the encrypted string to base L string. However, Leason discloses utilizing a method taught by Beach for generating and verifying a validation code as claimed (Leason: col. 12, lines 9-15; Beach: fig. 3; col. 6, line 56 – col. 8, line 32). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate Beach method into Leason. The motivation for doing so would have been to generate validation codes that are fraud resistant and without the need for a pre-approved database of valid validation codes (col. 5, lines 8-11).

Beach discloses using a checksum function to generate the validation number. Beach does not disclose using a one-way hash function with a first secret key. Schneier discloses using a one-way hash function with a first

secret key to generate a validation number having at least 16 bits (i.e., a MAC code) (pages 30-31, 455-459). It would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify Leason's method to use a one-way hash function with a first secret key to generate the validation number, as taught by Schneier. The motivation for doing so would have been that: (i) given a hash value, it would be computationally unfeasible to find a pre-image that hashes to that value (page 30, last paragraph); (ii) only someone with the secret key could verify the hash value (page 31, 2nd paragraph); and (iii) one could detect a single-bit change of the pre-image (page 30, last paragraph).

Regarding claims 14 and 32, Leason and Beach do not disclose that $n = 32$. However, the difference in length between the claimed value and the value of Beach is a matter of design choice. There is always a trade off when determining the number of bits designated for a value, i.e., the more bits designated, the more values can be assigned yet the longer time it takes to process the bits. The decision to select the number of bits for a value should be made based on the requirement of each system, and that number should vary from system to system. Therefore, it would have been obvious to one of ordinary skill in the art to modify Beach such that $n = 32$ if that were best for his/her system.

Regarding claim 24, Schneier further disclose using MD5 algorithm for the keyed-hash function (page 456, table 18.2).

11. Claims 13 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Leason in view of Beach and Schneier as applied to claims 12 and 22 above, and further in view of "FIPS 46-3". Beach discloses encrypting and decrypting the code (fig. 3, step 50). Beach does not disclose using the DES3 algorithm. "FIPS 46-3" discloses using the DES3 algorithm, i.e., Triple DES algorithm and 128-bit keys (Section 15 – Qualifications). It would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the combined method of Leason and Beach to use the DES3 algorithm for encryption and decryption, as taught in "FIPS 46-3", in order to increase data security (page 5, last paragraph).

Allowable Subject Matter

12. Claims 3, 21, 25, 33 and 37 are allowed over the prior art of record.

13. Claim 39 is objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

14. The following is a statement of reasons for the indication of allowable subject matter. Regarding claims 3, 21, 25, 33, 37 and 39, a 48-bit code comprising a 32-bit number and a 16-bit validation number has not been taught by prior art.

Conclusion

15. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number

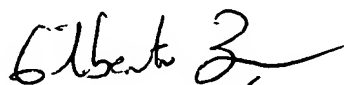
is 571-272-3802. The examiner can normally be reached on Mon-Fri:
10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/MD/
Minh Dinh
Examiner
Art Unit 2132

11/21/07


GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100